PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04K 1/00, H04L 9/00, 17/02 — A1

(11) International Publication Number: WO 95/26085

(43) International Publication Date: 28 September 1995 (28.09.95)

(21) International Application Number: PCT/US95/03578

(22) International Filing Date: 20 March 1995 (20.03.95)

(30) Priority Data:
08/210,200 18 March 1994 (18.03.94) US

(71) Applicant *(for all designated States except US)*: INNOVONICS, INC. [US/US]; Suite 200, 21644 N. Ninth Avenue, Phoenix, AZ 85027 (US).

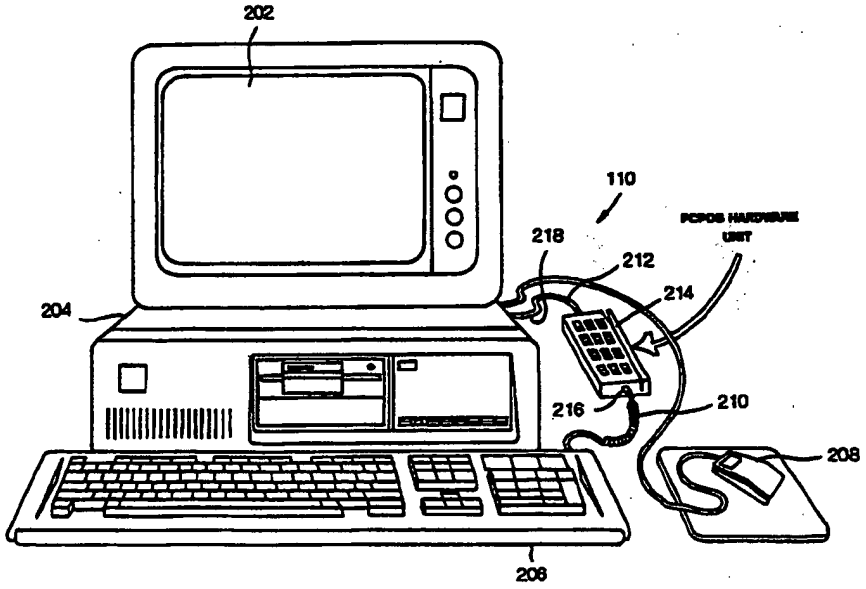
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: CLARK, Dereck, B. [US/US]; 3642 W. Camino Real, Glendale, AZ 85310 (US).

(74) Agents: KELLY, Michael, K. et al.; Snell & Wilmer, 400 East Van Buren, Phoenix, AZ 85004-0001 (US).

(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, MX, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SI, SK, TJ, TT, UA, US, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ, UG).

Published
With international search report.

(54) Title: METHODS AND APPARATUS FOR INTERFACING AN ENCRYPTION MODULE WITH A PERSONAL COMPUTER



(57) Abstract

An encryption module for encrypting financial and other sensitive data may be conveniently interposed in series between a personal computer and the keyboard associated therewith. An application program designed to run on the PC is configured to prompt the user to enter his PIN or other confidential data into the encryption module; consequently the confidential data need not be transmitted in an unencrypted fashion, and need not reside on the PC hard drive in an unencrypted form.

METHODS AND APPARATUS FOR INTERFACING AN ENCRYPTION MODULE WITH A PERSONAL COMPUTER

Technical Field

The present invention relates, generally, to methods and apparatus for remotely effecting financial transaction and, more particularly, to a technique for transmitting encrypted data to a host computer from a remote personal computer.

Background Art And Technical Problems

Systems for performing financial transactions from a remote location, e.g., the home, office, or retail facility, are becoming increasingly popular. The proliferation of personal computers, and particularly in conjunction with modems, permits a consumer to effect bill paying, retail purchasing, banking, and other commercial transactions remotely, thus avoiding the need to travel with an order to attend to routine commercial matters.

Presently known systems typically comprise a host computer located at a central data processing site, which is configured to communicate with a large number of remote personal computers (PC). When an individual desires to effect a financial transaction, for example to order merchandise and pay for the merchandise with a credit card, the user constructs a data link between his PC and the host computer via the PC's modem. Upon ordering the appropriate merchandise, the user may enter a credit card number corresponding to the account to which the merchandise is to be charged. The purchase request is then transmitted from the PC to the host computer, whereupon the transaction is verified by the host computer.

Presently known systems are limited, for example in their ability to effect the real time transfers of funds, due to various problems associated with the transmission of encrypted data. More particularly, real time transfer of funds are typically effected through the use of an automatic teller machine (ATM). In a typical ATM transaction, the user enters an account number onto a keypad or, alternatively, inserts a bank card into the ATM whereupon the account information is "read" from the magnetic strip located on the back of the bank card. Thereafter, the user enters a personal identification number (PIN) into the keypad to enable the transaction. By properly entering the PIN associated with the bank card, the fraudulent use of such cards is greatly reduced. The extension of the aforementioned ATM paradigm to home use is problematic, however, in that presently known systems for transmitting encrypted data (e.g. PINS) are unsatisfactory.

More particularly, although techniques for encrypting PINs and other confidential data and information are generally well known, current banking and other financial industry regulations are calculated to limit the extent to which confidential data may be transmitted in an non-encrypted form. In the context of a personal computer used to remotely effect a commercial transaction, it is possible

In accordance with the further aspect of the invention, the encryption module may be equipped with various peripheral devices useful in entering data and information, for example magnetic head card readers, "smart card" or integrated circuit card (ICC) readers, bar code readers, voice recognition devices, scanners, and the like. In this way, confidential data in virtually any medium may be entered into the encryption module and encrypted prior to subsequent processing and transmission, such that the potential for the unauthorized detection of the unencrypted data is minimized.

Brief Description Of The Drawing Figures

The present invention will hereinafter be described in conjunction with the 25 appended drawing figures, wherein like numerals designate like elements, and

Figure 1 is at schematic block diagram of a transaction authorization system in accordance with the present invention;

Figure 2 is a front elevation view of a personal computer having an encryption module integrated therewith;

Figure 3 is a schematic block diagram of an integral encryption module;

Figures 4 and 6-10 are flow charts setting forth the operation of an exemplary application program executed by the PC of figure 2 in accordance with the present invention;

Figure 5 is a display of various icons useful in conjunction with the software shown in figure 4;

Figure 11 is an alternate embodiment of the encryption module shown in figure 2;

Figure 12 is a schematic block diagram of the functional aspects of the encryption module of figure 2;

Figure 13 is a schematic circuit diagram of the processor embodied in the encryption module of figure 2;

Figure 14 is a schematic circuit diagram of the keypad shown in Figure 2; Figure 15 is a schematic circuit diagram of an analog switch used in the encryption module of the present invention;

Figures 16 and 17 are schematic circuit diagrams of a magnetic strip reader circuit;

Figures 18-20 are schematic memory maps of various memory sectors associated with the processor of figure 13; and

Figures 21-36, are flow chart diagrams setting forth various functional features of the encryption module of the present invention.

Detailed Description of Preferred Exemplary Embodiments

Referring now to Figure one, a remote transaction system 100 suitably comprises a host computer system 102 which may be interfaced with one or more transaction networks, for example a bill paying network 104, a banking system network 106, and various other network systems 108,

With momentary reference to Figure 3, yet a further alternative embodiment suitably comprises a self contained, integral module 300 including at screen 306, a computer 304, a keyboard 302, a modem connection 308, and an accessory connector 310 for interfacing module 300 with various preferred devices, for example bar code readers, smart card readers, magnetic strip readers and the like. In accordance with the embodiment in Figure 3, only those components necessary to effect the specific functions discussed need be incorporated into module 300 resulting in substantial cost savings over the PC embodiment shown in Figure 2. However, it will be appreciated that, for those consumers who already own a PC, the embodiment illustrated in Figure 2 may be preferable in as much as a conventional PC may be readily adapted in accordance with the present invention by incorporating module 214 into PC 110.

Referring now to Figures 4-10, an exemplary remote transaction application program useful in accordance with the present invention will now be described.

Particular reference to Figure 4, a suitable application program may be executed using a (WINDOWS) format which presents the user with various menu selections. Those skilled in the art will appreciate that the use may select various options using keyboard 206 or mouse 208 (see Figure 2) as is known in the art. Although the subject application program is described herein in the context of the WINDOWS embodiment, it will be appreciated that the subject invention may be implemented in the context of any convenient applications environment.

With continued reference to Figure 4, upon activating the WINDOWS capability of PC 110 (Step 402), the user may select one of a plurality of menu options 406-416, for example by double clicking mouse 208 (Step 404). More particularly and with momentary reference to Figure 5, the user may select banking operation 406 corresponding to icon 506, a bill paying operation 408 represented by icon 508, a neighborhood shopping operation 410 represented by icon 510, a mail ordering operation 412 represented by icon 512, a state lottery operation 414 represented by icon 514, a file operations 416 corresponding to 516, at PC setup operation 418 corresponding to icon 518, a hardware test operation 420 corresponding to icon 520, a display time operation 422 corresponding to Icon 522, or a tutorial operation 424 represented by icon 524. Although the illustrated icons shown in Figure 5 are useful in the context of the illustrated embodiment, it will be appreciated that any suitable Icon or other mechanism for selecting various program options may be employed in the context of the present invention. Moreover, the menu options set forth in figures A and 5 are merely exemplary; various combinations of the menu options shown in the figures, alone or in combination with other menu options not set forth herein may also be employed in the context of the present invention.

With continued reference to Figure 4, tutorial operation 424 suitably entails an explanation of the various menu options and an explanation of how to use the options. Display time option 422 suitably displays the system time in any desired format. Hardware test operation 420 is suitably

Referring now to figures 6 and 7, funds transfer operation 602 suitably entails a selection of a particular bank account (Step 610), for example a savings account, checking account, money market account, and the like. When the account which the user desires to debit is selected, the system suitably prompts the user to enter an amount which is to be transferred or paid (Step 702), for example by entering an amount into PC 110 via keyboard 206 (704). If no amount is entered after a predetermined time or if an incorrect amount (e.g. "zero", a negative amount, or an amount which exceeds the predetermined threshold), the system may resume its previous processing path (Step 706). If a correct amount of funds to be paid or transferred is entered by the user, the user may be suitably prompted to select the method of payment (Step 708), whereupon a transaction request is suitably transmitted from PC 110 to module 214 (Step 710), as discussed in greater detail below.

In accordance with one aspect of the present invention, it may be desirable to permit particular transactions, e.g. transactions involving the transfer of money, only upon the satisfaction of certain threshold conditions. For example, it may be desirable to permit a funds transfer only if a receipt evidencing the transaction may be printed at a printer which is located proximate PC 110.

More particularly and with continued reference to Figure 7, the system may be suitably configured to confirm: (1) whether PC 110 is equipped with or otherwise has access to a local printer; (2) that the aforementioned printer is equipped with paper upon which a receipt may be printed (Step 712).

If PC 110 either does not have a printer associated with it or if it has a printer but the printer it out of paper, the system may prompt the user to install an appropriate printer and/or paper (Step 714), whereupon the system again checks to confirm the presence of a functional printer (Step 718). If a functional printer still is not detected, an appropriate error message is generated.

If it is determined that PC 110 has a functioning printer (loaded with paper) associated therewith, PC 110 is suitably configured to transmit a command to module 214 which causes module 214 to enter a "swipe" mode of operation (Step 716), discussed in greater detail below in conjunction with figures 27 and 28. The user may thereafter enter the appropriate account data, for example by swiping a transaction card through a magnetic card reader, entering a smart card into a smart card reader associated with PC 110 entering account data via keyboard 206, or any other convenient mechanism for entering account data associated with PC 110 or modem 214 (Step 720).

Referring now to Figure 8, once the account data is entered, PC 110 may suitably be configured to display the account data on screen 202 (Step 802). The particular transaction being performed by the user is of a type which does not require the transmission of confidential data (e.g. PIN), the account data and the funds transfer/bill payment data discussed above may be assembled and transmitted to host computer 102 via data link 118 for processing (Step 812). "If, on the other hand, the particular transaction requires the entry of confidential information, the system may be suitably configured to prompt the user to enter such confidential information (Step 804).

system way be configured to require a functioning printer as a prerequisite to effecting the foregoing smart card updating function, as desired.

If, on the other hand, the user desires to "withdrawal" funds from the smart card (Step 904), the system may prompt the user to select the destination of the funds withdrawn from the smart card (Step 906), and to request the user to enter a PIN or other confidential data (Step 908). In this regard, the entry of such confidential information is suitably effected in a manner analogous to that described below in conjunction with figures 11, 14, and 25-28. Upon entry of the PIN, the smart card transaction may be suitably affected via the smart card reader/writer circuit (not shown) associated either PC 110 or module 214.

Referring once again to Figure 4, upon the selection of bill paying operation 408, the system may be configured to prompt the user to add a new bill to the bill paying operation (Step 1002). More particularly, the bill paying function of the subject system suitably entails a method of keeping track of various bills, for example department store bills, credit card bills, utility bill, and the like in conjunction with PC 110. If the user desires to add a new billing entity to the billing operation, for example a new department store charge account, the data corresponding to the new account may be entered into PC 110 by the user (Step 1008), for example via keyboard 206.

The system may be further configured to display various bills comprising billing operation 408 (Step 1004), permitting the user to either exit to the main menu (Step 1010) or, alternatively, to select a particular bill for payment (Step 1006). Once a particular bill is selected for payment, the system is suitably configured to effect payment of the bill in accordance with the Steps described upon in conjunction with Figure 7.

It will appreciated at various times during the execution of the foregoing application program, the users require to enter various account, PIN, and other information and/or data into the system, for example via module 214. Thus, in accordance with one aspect of the present invention, module 214 may be suitably configured to assume a plurality of different modes, depending on the particular function then being effected. The circuitry comprising module 214 which permits module 214 to assume these various operational states will now be described, followed by a functional description of the various operation modes associated with module 214.

With momentary reference to Figure 11, module 214 may suitably assume any desired configuration, for example the sloping, contoured embodiment shown in Figure 11. In particular, module 214 suitably comprises a housing 1100, for example an injection molded plastic housing similar to the conventional "mouse" typically employed in conjunction with personal computers. In accordance with the embodiment shown in Figure 11, module 214 suitably comprises a keypad 1102, for example corresponding to the numbers 0-9, and further including inter alia, various functional, for example an enter (E) and cancel (C) button. Module 214 further comprises a card reader slot 1104

pd0, pd1	interface to pentec bar code reader data loader
pd2	pc clock
pd3	pc data
pd4	keyboard clock
pd5	keyboard data
pe0	keypad column 1
pe1	keypad column 2
pe2	keypad column 3

Referring now to figures 12-14, keypad 1102 is suitably connected with the various ports associated processor 1212 as set forth in Figure 14.

Refer now to figures 12-13 and 15, control gate 1222 suitably comprises an analog switch, for example a module no. 74HC4066 manufactured by Motorola, Inc. Switch 1222 suitably comprises four internal switches a-d, which are suitably simultaneously controlled by the output of port pb4, such that internal switches a-d are either all open or all closed in accordance with the logic value of the output of port pb4. Generally speaking, in essentially all operational states of module 214, internal switches a-d will remain open, effectively isolating keyboard 206 from box 204. During the transparent mode (discussed below), internal switches a-d will typically remain closed, permitting normal communication between the keyboard and the PC.

With continued reference to Figures 12-13 and 15, the buffer enable signal from port pb4 of processor 1212 is suitably applied to control gate 1222. In additional the keyboard clock and keyboard data signals are transmitted between ports which pd4 and pd5, respectively, of microprocessor 1212 to a databus 1219 extending from switch 1222 to keyboard 206 via connector 210. Similarly, the PC clock and PC data signals are transmitted between ports pd2 and pd3, of microcontroller 1212 to a databus 1218 extending between control gate 1222 and box 204 (Figure 1) via connector 212.

Referring now to figures 12, 13 and 16, a first embodiment of magnetic Stripreader circuit 1206 associated with magnetic strip reader 1104 (Figure 11) suitably comprises a magnetic reader head 1602, for example a 1.6 microhenry inductor coil, respective first and second amplifiers 1604 and 1606, for example model no. LM324a operational amplifiers, respective comparators 1608 and 1610, for example model no. LM393, and an inverting schmidt trigger 1612, for example 74HC14.

More particularly and with continued reference to Figure 16, a transaction card of the type bearing a magnetic strip is Suitably slid through magnetic strip reader 1104 of module 214 (Figure 11) such that the magnetic strip magnetically engages reader head 1602. The output of coil 1602 is suitably applied to the inverting input of amplifier 1606 which suitably exhibits a gain on the order of 20. The output of amplifier 1604 is suitably applied to the noninverting input of amplifier 1606. The output of amplifier 1606 is suitably applied to the noninverting input of comparator 1608 and to the inverting input of comparator 1610. By applying a determined threshold voltage to the inverting input of amplifier 1608, and by, also applying a predetermined threshold voltage to the non-inverting input of amplifier 1610, a series of logic hi and logic low pulses are applied to the input of

present invention which provides adequate security against unauthorized detection of the underlying confidential data.

Referring now to figures 21-38, the operation of system 100, and particularly the operational states of module 214, will now be described.

With particular reference to Figure 21, upon powering up of module 214, a reset signal is applied to reset port 1310 of processor 1212 (Step 2102).

Upon entering the reset condition, system initialization is executed (Step 2104).

More particularly and with momentary reference to Figure 22, system initialization Step 2104 suitably entails various initialization Steps (2104b), Including, inter alia:

1. Initializing the current mode to transparent mode, for example by setting current mode, register 1804 (see Figure 18) to the transparent mode condition, as discussed in greater detail below;
2. Initializing previous mode register 1806 to "no mode";
3. Initializing the system Interrupts to appropriate trigger characteristics;
4. Enabling interrupts from the PC interface bus (e.g. connector 212); and
5. Initializing the PC interface temporary buffer 1808 to "empty". The relevancy of the foregoing initialization steps are discussed in greater detail below in conjunction with ensuing description of the operation of module 214.

Upon completing system initialization, the system enters a system redirect state (Step 2106), whereupon the system then enters the appropriate operational mode; in the context of system startup, the system will default to transparent mode, as set forth above in conjunction with system initialization Step 2104(b).

More particularly, a preferred embodiment of the present invention employs an interrupt-based processing scheme within module 214. Thus, as the system flows through the main operational loop set forth in Figure 21, the system will from time to time receive interrupts from PC 110. Upon receipt of a "mode change" interrupt command from PC 110, processor 1212 causes Module 214 to terminate the then current mode, and enter system redirect (Step 2106), from which the appropriate new operational mode may be entered.

From the main control loop governing the operation of module 214 shown in Figure 21, the system may enter any one of a number of operational states as a result of a number of predicate instructions. More particularly, the system may enter certain operational states as controlled by the executable code resident within sector 1904 of ROM 1902. In addition, the system may enter certain operational states as a result of commands received from PC 110, as set forth in more detail in conjunction with Figure 23.

Referring now to Figure 23, PC 110 from time to time sends interrupt commands to module 214 via connector 212 (Step 2302).

More particularly, and with reference to figures 12, 13, and 15, Step 2410 of Figure 24 suitably entails processor 1212 generating a buffer enable signal at port PB4, and transmitting the buffer enable signal to control gate (switch) 1222. In response, internal switches A-D of switch 1222 are closed, establishing direct communication between PC 110 and keyboard 206 through connector 212, BUS 1218, switch 1222, BUS 1219, and connector 210. Thereafter, the system continues to cycle through transparent mode 2110, permitting normal operation of keyboard 206 with respect to PC 110. The system will continue to cycle through transparent mode 2110 until a subsequent message is received from PC 110.

Returning now to Figure 21, the system way also receive a command to enter scan mode (Step 2112), for example in response to a scan mode request from PC 110 (see Step 806, Figure 8), whereupon processor 1212 causes module 214 to enter the scan mode of operation (Step 2114).

More particularly and referring now to Figure 25 (scan mode 2114) generally involves "scanning" the circuitry associated with keypad 1102 (Figure 14) to detect data (e.g. PIN) entered into keypad 1102 by the user.

With continued reference to Figure 25, scan mode operation Involves, inter alia, initializing PIN entry buffer 1814 of RAM 1802 to empty (Step 2502), to prepare the PIN buffer to receive data which is about to be entered onto keypad 1102 by the user.

The system detects whether a subsequent mode change command has been received (Step 2504); if so, the system returns to system redirect Step 2104. If no mode change has occurred, module 214 waits until a keypress is detected (Step 2506) or, alternatively, until a mode change is detected (Step 2504).

More particularly, processor 1212 scans ports PB0-PB3 and ports PE0-PE2 (See Figure 13) corresponding to rows 1-4 and columns 1-3 of keypad 1102, respectively (See Figure 14). When a keypress is detected, the system determines if the depressed key corresponds to one of the numbers 0-9 (Step 2508); if so, module 214 suitably sends a signal to PC 110 to cause a "dummy" indicia of the depressed key to screen 202 (Figure 2).

More particularly, the operational program stored in sector 1904 of ROM 1902 (Figure 19) of processor 1212 suitably includes operating code which permits module 214 to communicate with PC 110 in a manner which emulates the manner in which conventional keyboards (e.g. keyboard 206) typically communicate with box 204. In a preferred embodiment of the present invention, the operating code governing the operation of module 214 is suitably configured in accordance with any suitable protocol, for example the protocol employed by IBM in its PCs or any other suitable derivative or variant thereof, to thereby permit module 214 to communicate with box 204 in a manner which emulates conventional communication between keyboard 206 and box 204, data transmission and other communication between module 214 and box 204 may be conveniently and efficiently carried out in a manner which is essentially transparent to box 204; that is, when box 204 receives data

2602). These data, alone or in conjunction with other data, are suitably combined and encrypted in any suitable matter (Step 2602). In a preferred embodiment, these data may be suitably combined in accordance with ANSI specification X9.24-1992. The data is suitably encrypted in accordance with ANSI standard X3.92-1981 or any other desired encryption technique. More particularly, the foregoing combination and encryption algorithms are desirably resident in operational program sector 1904 of ROM 1902, and operate in conjunction with encryption key information suitably stored in EEPROM 2002 (See figures 19 and 20). By storing the encryption key data in nonvolatile memory (i.e., EEPROM), system integrity and security is enhanced.

With continued reference to Figure 26, upon encrypting the data in accordance with Step 2602, the encrypted data is suitably written into the next successive location in encrypted PIN sector 1816 of RAM 1802 (Step 2604). Thereafter, the address corresponding to the location in sector 1816 wherein the encrypted data is written is transmitted to PC 110 (Step 2606). More particularly, and with momentary reference to Figure 2, once the data is encrypted within module 214, the location of the encrypted data is transmitted to PC 110 via connector 212, such that unencrypted confidential data need not be transmitted from module 214 to PC 110 in order to effect a transaction.

After encrypting the data, processor 1212 suitably creates a new unique key for use in a subsequent encryption process and stores the new key in future encryption key sector 2004 of EEPROM 2002 (Step 2608). In accordance with one aspect of the present invention, the new encryption key may be generated in accordance with any suitable scheme which is compatible with the encryption algorithm executed in Step 2602. In accordance with a preferred embodiment, a new unique encryption key may be generated in accordance with ANSI X9.24-1992.

Upon transmitting indicia of the encrypted data from module 214 to PC 110, PC 110 continues to execute the application program residence therein, as described above in detail in connection with figures 4-10.

Returning now to the main control loop 2100 of module 214 (Figure 21), module 214 may also elect to enter card swipe mode 2118 (Step 2116). More particularly, and with momentary reference to Figure 7, PC 110 may request Module 214 to enter the card swipe operational mode, for example at a point during the execution of the application software resident in PC 110 where such application software prompts the user to swipe his transaction card through card swipe slot 1104 of module 214 (Figure 11), for example as discussed above in connection with Step 716.

Referring now to Figure 27, upon entering the swipe operational mode, processor 212 suitably initializes (clears) respective swipe data input buffers 1820, 1822 of RAM 1802 (Step 2702). The system then looks for a mode change (Step 2704), and returns to system redirect state 2106 if a mode change is detected. Otherwise, the system sets a swipe timeout counter to a predetermined maxtime during which the transaction must engage the card reader (Step 2706). In a preferred embodiment, the

of time, for example ten milliseconds to one second, as a card is drawn through card reader slot 1104 (Figure 11).

Returning now to Figure 21, module 214 is also configured to enter print mode 2122 from main loop 2100 (Step 2120) for example upon a request to do so from PC 110 (see Step 816, Figure 8).

Referring now to Figure 29, print operation mode 2122 suitably entails initializing the printer (Step 2902), for example to establish various hardware and software parameters associated with the printing process. In this regard, and as briefly discussed above, the printer may be affiliated with PC 110, for example by connecting a printer directly to box 204, or by connecting the printer to PC 110 via a suitable networking configuration. Alternatively, the printer may interface directly with the encryption module, for example at connector 310 of module 300 (Figure 3 or, alternatively, at peripheral device module 1200 of module 214 as shown in Figure 12.

With continued reference to Figure 29, the system determines if a mode change has occurred (Step 2904) and, if so, returns to system redirect Step 2906.

The system then determines if the data to be printed is currently available, for example by interrogating data output buffer 1810 (Figure 18) (Step 2908). If the data is not available, the system returns to Step 2902 to await the data to be printed. If the data is available ("yes" branch of Step 2908), the system determines if the printer is ready (Step 2930). In this regard, the printer to be checked will likely be connected to module 214, inasmuch as it would not typically be necessary to execute print operation 2122 if the printer were connected to PC 110. Stated another way, if PC 110 is equipped with a printer, the print operation may be controlled directly by PC 110, while the print operation as set forth in Figure 29 is appropriately controlled by module 214 if the printer employed in the context of the present invention is interfaced with module 214.

With continued reference to Figure 29, if the printer is not ready, module 214 suitably sends a command to the PC indicating that the printer associated with module 214 is not ready. In this regard, PC 110 may prompt the user to correct the printer situation, for example as described above in conjunction with Figure 7.

If the printer associated with module 214 is ready, the data resident in data output buffer 1810 is transmitted to the printer, for example via serial bus 1211 (see Figure 12). In accordance with the preferred embodiment, the data to be printed is transmitted to the printer in serial fashion; hence, the process set forth in Figure 29 is desirably repeated until the data present in data output buffer 1810 is sequentially transmitted to the printer.

Returning now to main loop 2100 (Figure 21) and with reference to Figure 30, module 214 is suitably configured to enter modem mode 2126 (Step 2124), for example in response to a request to do so from,PC 110 (see Step 710, Figure 7).

Referring now to figures 21 and 32, module 214 may be suitably configured to enter bar code operational mode 2130 (Step 2128), for example in response to a request to do so from PC 110. Bar code operation 2130 suitably entails determining whether a mode change has occurred (Step 3302) and, if so, returning to system redirect Step 2106. If a mode change has not occurred, data may be input from a general purpose module 1210, for example a bar code reader (Step 3204). Once the bar code or other data is received by module 214, it may be appropriately transmitted to PC 110, as desired (Step 3206).

Referring now to figures 21 and 33, module 214 may be suitably, configured to execute a smart card operation 2134 (Step 2132), for example in response to a request from PC 110 to do so. In this regard, although many of the various functional features associated with module 214 (e.g. modem operation 2126, print operation 2122, swipe operation 2118, and the like) are initiated in response to a request from PC 110 in accordance with the embodiment described herein, it will be appreciated that the various operational states of module 214 may suitably be effected in any desired manner, for example by entering appropriate commands directly into module 214.

With continued referenced to Figure 33, smart card mode 2134 suitably details determining whether a mode change has occurred (Step 3302) and, if so, returning to system redirect Step 2106.

If no mode change has occurred, the system determines if data is to be read from a smart card (Step 3304). In this regard, and as briefly stated above, such a request may come from PC 110, or may be otherwise effected by the user, for example by entering a particular code or depressing other buttons (not shown) onto keypad 1102 (Figure 11).

If data is to be read from a smart card ("Yes" branch of Step 3304), data is retrieved by processor 1212, for example via smart card, reader 1208 (Figure 512). Upon retrieving the data from the smart card, the data may be transmitted to PC 110 (Step 3306).

As discussed above, module 214 may also be configured to write data onto a smart card. In this case, the appropriate data to be written into the smart card may be suitably retrieved from data output buffer 1810 and applied to smart card circuit 1208 (Steps 3308, 3310).

Referring now to figures 21 and 34, module 214 in the PC application software discussed above in conjunction with figures 410 may be suitably configured such that the application software resident in PC10 must first validate module 214 before permitting the transmission of encrypted data or otherwise performing functions described herein. More particularly, in view of the importance of maintaining security in the context of real time funds transfer authorization, it may be desirable to permit PC 110 (e.g., through software) to confirm that module 214 embodies satisfactory security features before effecting transactions.

With continued reference to figures 21 and 34, module 214 may be suitably configured to enter a system validation mode 2138 (Step 2136), for example in response to a request from the user or from PC 110 to do so. System validation mode 2138 entails, inter alia, a determination of whether a mode

CLAIMS:

1. A remote processing system, located at a first site, for interfacing with a host computer system located at a second site which is remote from said first site, the host computer system being of the type which includes a host modem and which is configured to facilitate financial transactions upon receipt from said remote processing system of a data packet including an encrypted data field, said remote processing system comprising:

a. PC, comprising:

(1) a first memory sector configured to store an interactive software program;

(2) a first processor configured to execute said software program;

(3) an input port configured to communicate with said first processor and

(4) a second modem configured to transmit said data packet from said PC to the host modem in accordance with said software program; and

b. an encryption module, comprising:

(1) a keypad;

(2) a second processor configured to encrypt data entered onto said keypad; and

(3) a data link configured to maintain communication between said encryption module and said PC input port.

2. The remote processing system of Claim 3, wherein said input port comprises a keyboard input port.

3. The remote processing system of Claim 3, wherein said input port comprises a mouse port.

4. The remote processing system of Claim 4, wherein said PC further comprises a keyboard, and said encryption module is connected in series between said keyboard and said keyboard input port.

5. The remote processing system of Claim 4, wherein said second processor is configured to transmit said encrypted data to said input port in a manner which emulates the transmission of keyboard input data.

6. The remote processing system of Claim 3, wherein said data entered onto said keypad corresponds to a PIN.

7. The remote processing system of Claim 3, wherein said PC further comprises a screen, and said first processor is configured to generate a data entry prompt on said screen in accordance with said software program.

(2) a first processor, disposed within said PC housing, configured to execute a software program;

(3) an input port accessible from outside of said PC housing and configured to communicate with said first processor; and

(4) a PC modem configured to transmit said data packet from said PC to the host modem in accordance with said software program; and

b. an encryption module, comprising:

(1) a module housing;

(2) a keypad accessible from outside of said module housing;

(3) a second processor disposed within said module housing and configured to encrypt data entered onto said keypad; and

(4) a data link configured to maintain communication between said encryption module and said PC input port.

19. The remote processing system of Claim 20, wherein:

a. said input port comprises a keyboard input port;

b. said PC further comprises a keyboard, and said encryption module is connected in series between said keyboard and said keyboard input port; and

c. said second processor is configured to transmit said encrypted data to said input port in a manner which emulates the transmission of keyboard input data.

20. A data encryption terminal of the type comprising a single, unitary housing, a keypad circuit disposed within said housing and connected to a keypad which is accessible from outside of said housing, processing circuitry configured to execute a software application program and to encrypt data entered on said keypad, and a modem for transmitting said encrypted data from said terminal, the improvement comprising:

a. a first housing, within which is disposed said modem and a first processor for executing said software application program; and

b. a second housing, separate from said first housing, within which is disposed a said keypad circuit and a second processor configured to encrypt data entered on said keypad.

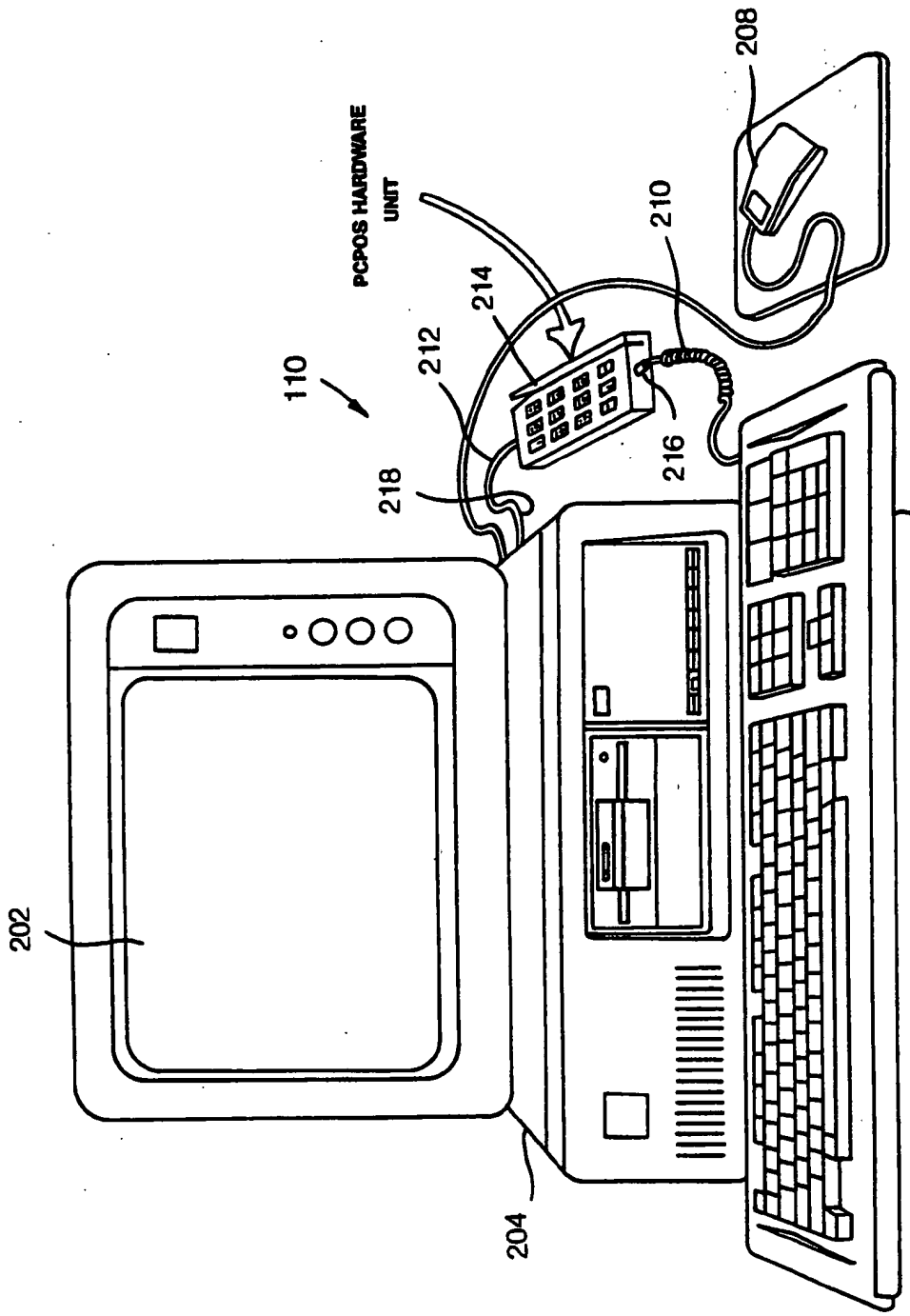
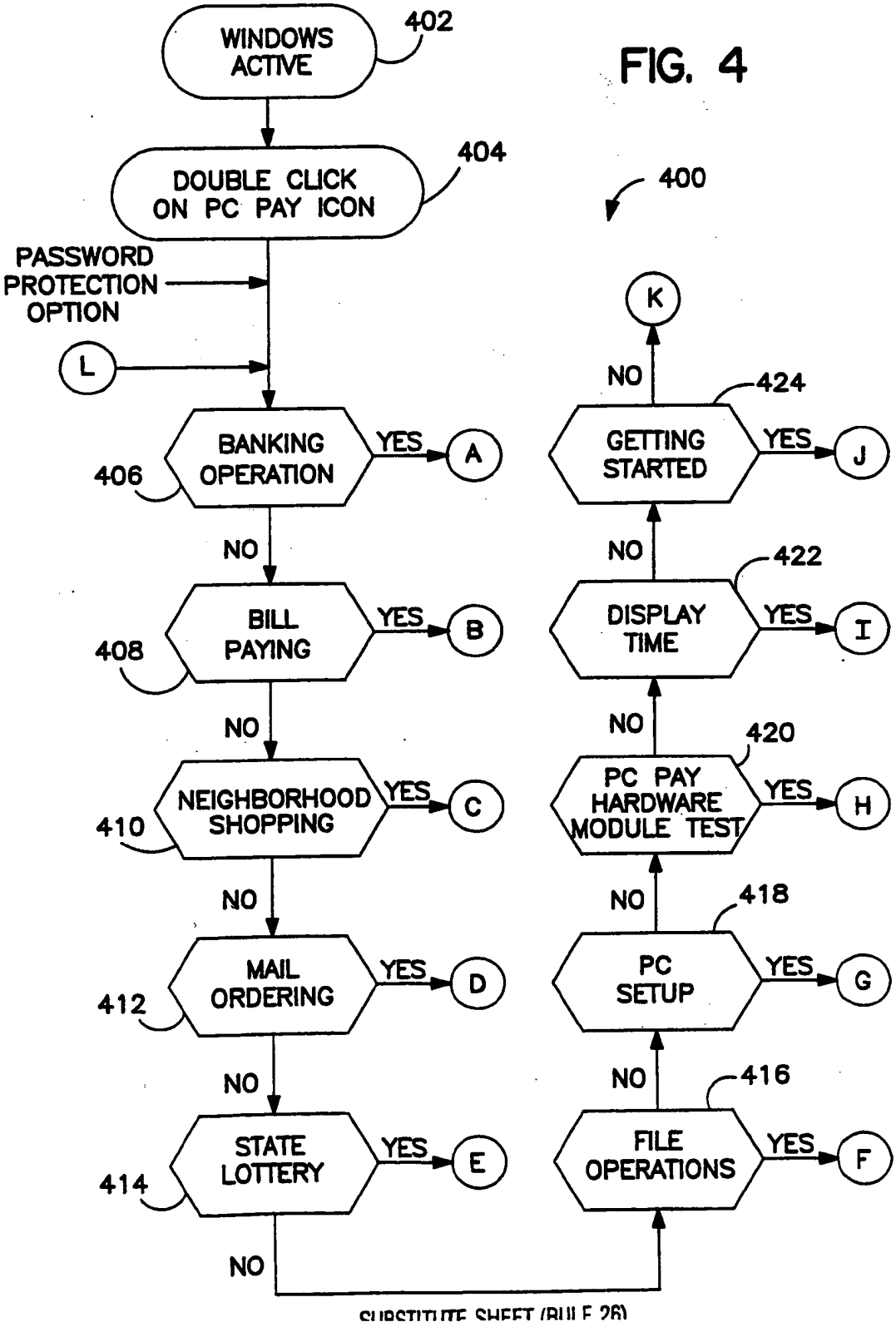


FIG. 2

FIG. 4


WINDOWS ACTIVE
402
DOUBLE CLICK ON PC PAY ICON
404
400
PASSWORD PROTECTION OPTION
L
BANKING OPERATION
406
YES
A
NO
BILL PAYING
408
YES
B
NO
NEIGHBORHOOD SHOPPING
410
YES
C
NO
MAIL ORDERING
412
YES
D
NO
STATE LOTTERY
414
YES
E
NO
K
NO
GETTING STARTED
424
YES
J
NO
DISPLAY TIME
422
YES
I
NO
PC PAY HARDWARE MODULE TEST
420
YES
H
NO
PC SETUP
418
YES
G
NO
FILE OPERATIONS
416
YES
F

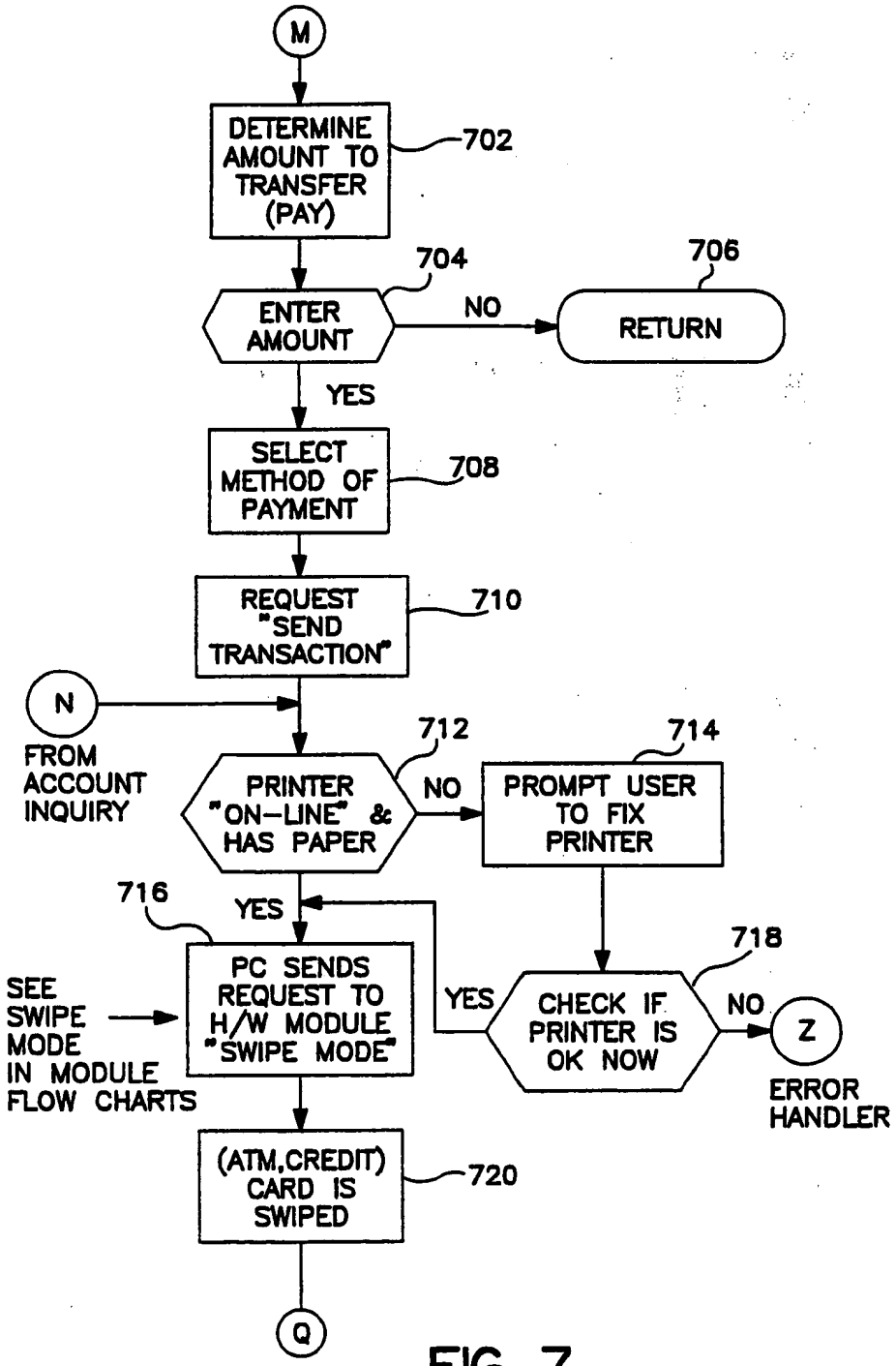

M
DETERMINE AMOUNT TO TRANSFER (PAY)
702
704
ENTER AMOUNT
NO
706
RETURN
YES
SELECT METHOD OF PAYMENT
708
REQUEST "SEND TRANSACTION"
710
N
FROM ACCOUNT INQUIRY
712
PRINTER "ON-LINE" & HAS PAPER
NO
714
PROMPT USER TO FIX PRINTER
716
YES
PC SENDS REQUEST TO H/W MODULE "SWIPE MODE"
SEE SWIPE MODE IN MODULE FLOW CHARTS
YES
718
CHECK IF PRINTER IS OK NOW
NO
Z
ERROR HANDLER
(ATM,CREDIT) CARD IS SWIPED
720
Q

FIG. 7

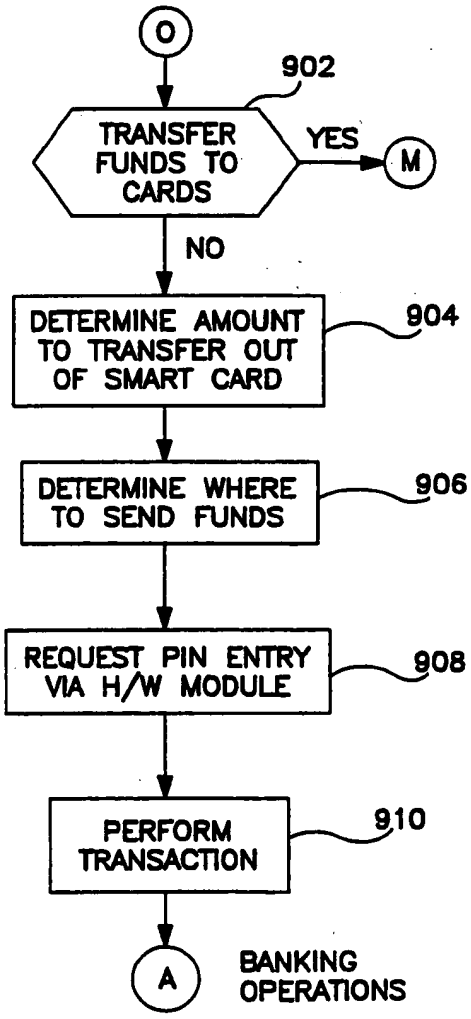

O
902
TRANSFER FUNDS TO CARDS
YES
M
NO
DETERMINE AMOUNT TO TRANSFER OUT OF SMART CARD
904
DETERMINE WHERE TO SEND FUNDS
906
REQUEST PIN ENTRY VIA H/W MODULE
908
PERFORM TRANSACTION
910
A
BANKING OPERATIONS

FIG. 9

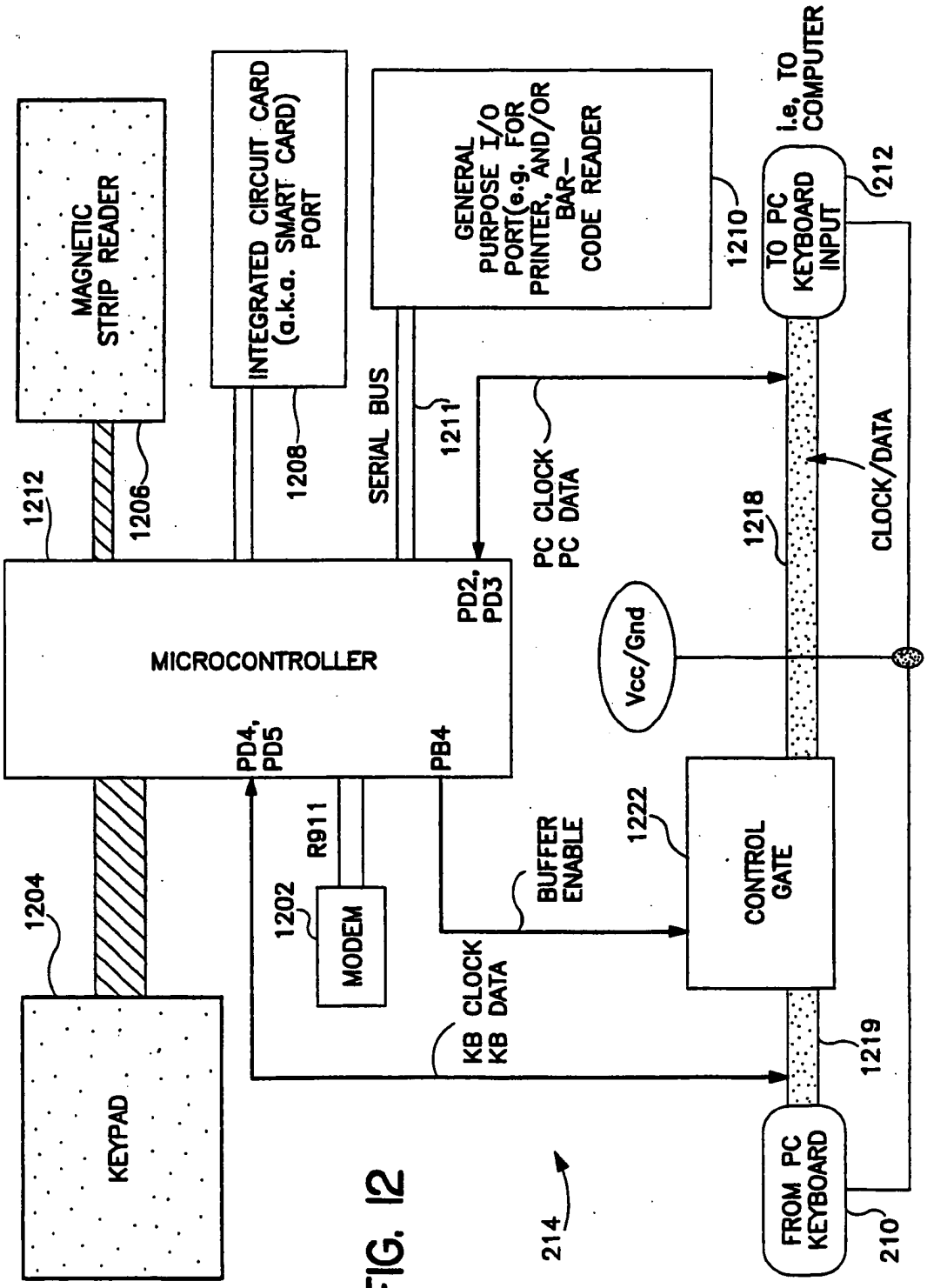

MAGNETIC STRIP READER
INTEGRATED CIRCUIT CARD (a.k.a. SMART CARD) PORT
GENERAL PURPOSE I/O PORT(e.g. FOR PRINTER, AND/OR BAR-CODE READER
1210
i.e, TO COMPUTER
TO PC KEYBOARD INPUT
212
1212
1206
1208
SERIAL BUS
1211
PC CLOCK
PC DATA
1218
CLOCK/DATA
PD2, PD3
MICROCONTROLLER
Vcc/Gnd
PD4, PD5
PB4
R911
1202
MODEM
BUFFER ENABLE
1222
CONTROL GATE
1204
KB CLOCK
KB DATA
1219
KEYPAD
FROM PC KEYBOARD
210
214

FIG. 12

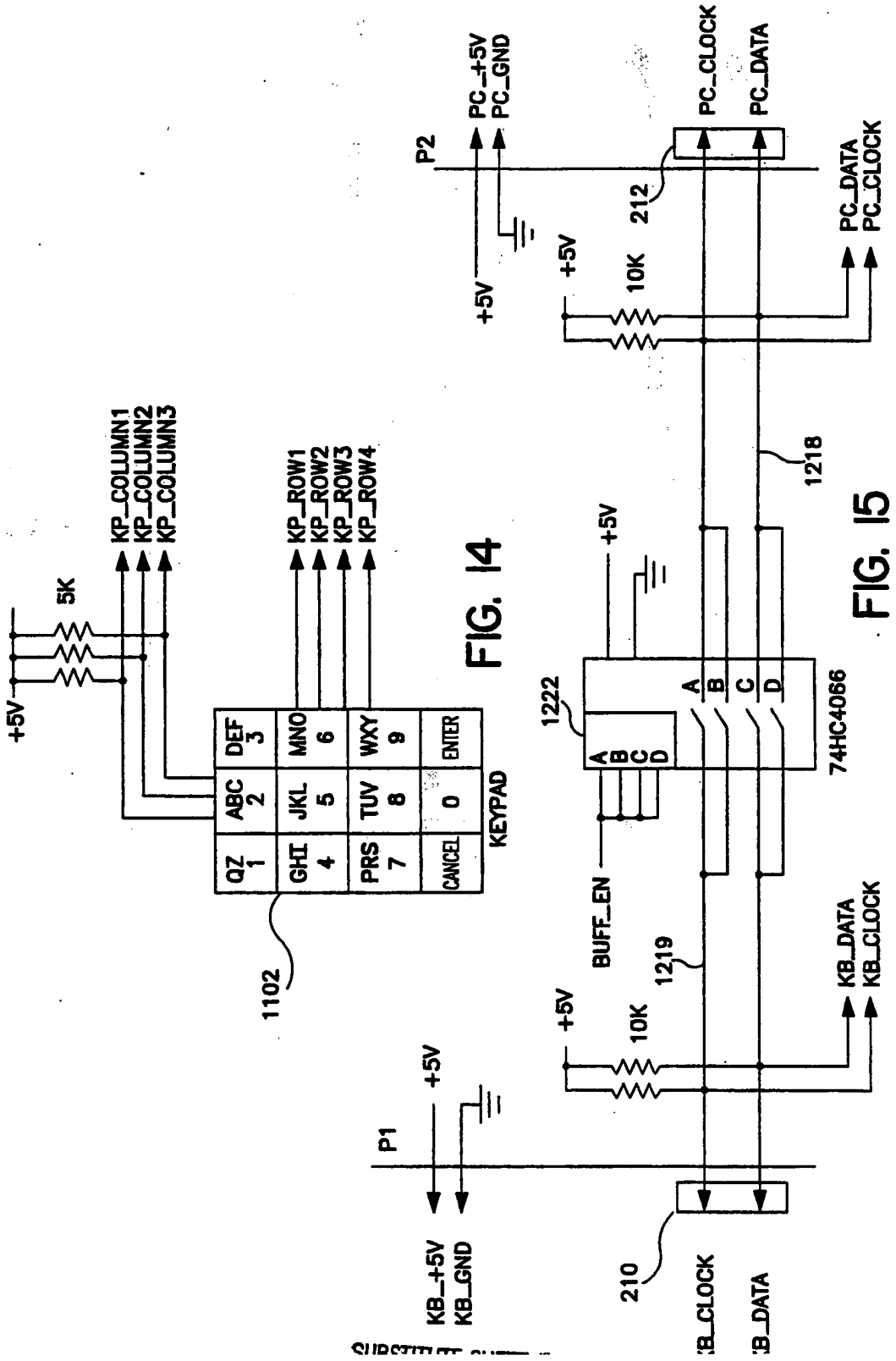

P2
PC_+5V
PC_GND
PC_CLOCK
PC_DATA
212
+5V
10K
PC_DATA
PC_CLOCK
1218
+5V
1222
A
B
C
D
74HC4066
BUFF_EN
1219
+5V
10K
KB_DATA
KB_CLOCK
P1
+5V
KB_+5V
KB_GND
210
KP_COLUMN1
KP_COLUMN2
KP_COLUMN3
KP_ROW1
KP_ROW2
KP_ROW3
KP_ROW4
5K
+5V
QZ 1
ABC 2
DEF 3
GHI 4
JKL 5
MNO 6
PRS 7
TUV 8
WXY 9
CANCEL
0
ENTER
KEYPAD
1102

FIG. 14

FIG. 15

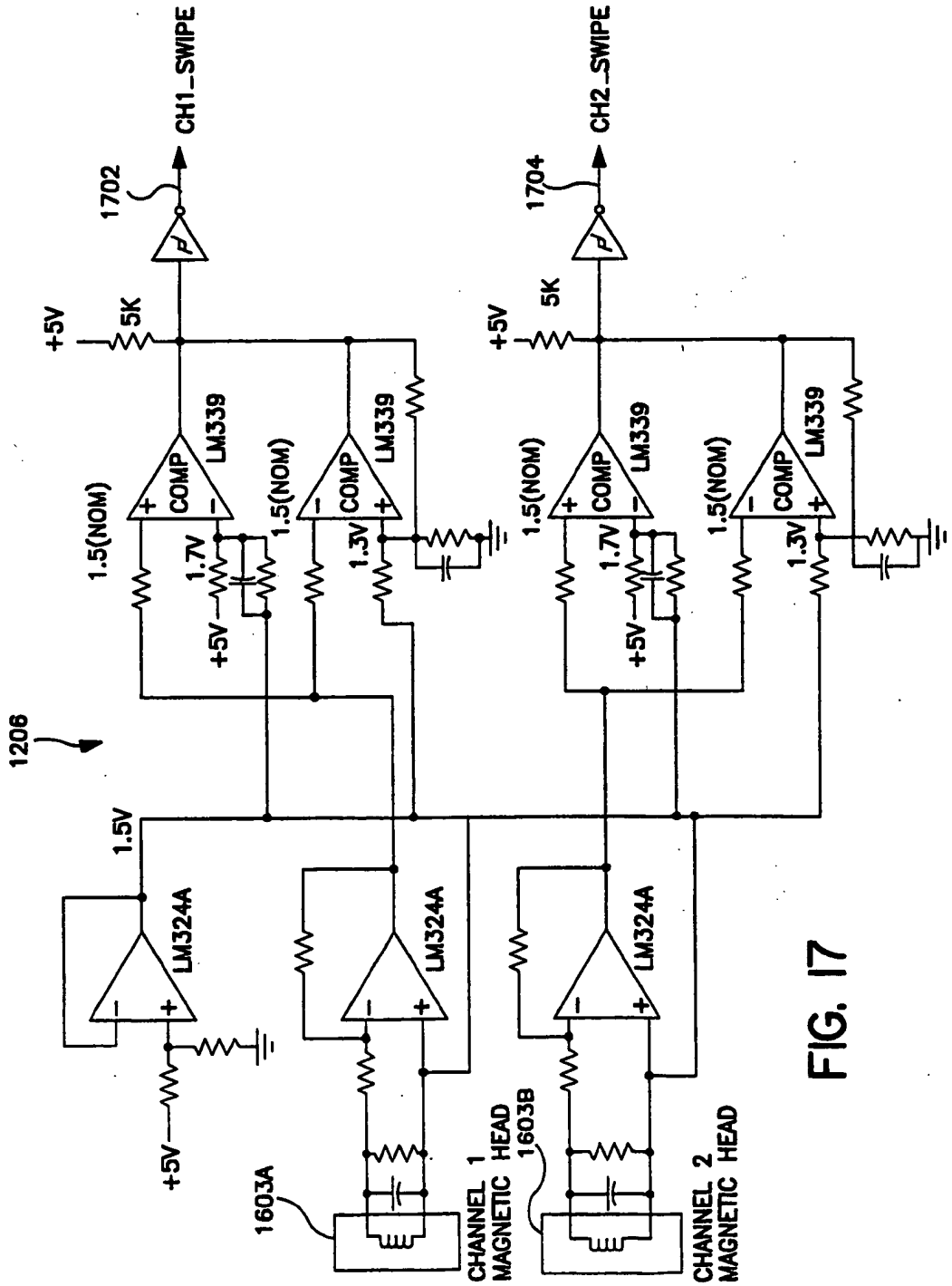

CH1_SWIPE
CH2_SWIPE
1702
1704
+5V
5K
LM339
COMP
1.5(NOM)
1.7V
1.3V
1206
1.5V
LM324A
1603A
1603B
CHANNEL 1 MAGNETIC HEAD
CHANNEL 2 MAGNETIC HEAD

FIG. 17

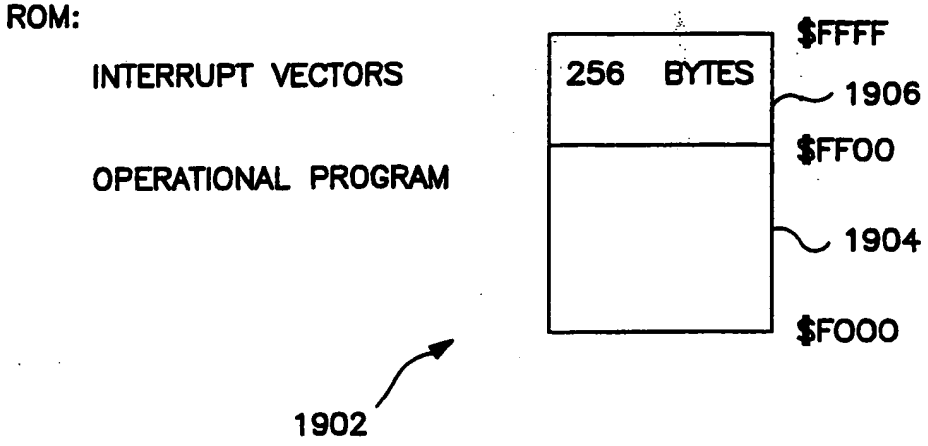

ROM:
INTERRUPT VECTORS
OPERATIONAL PROGRAM
256 BYTES
$FFFF
1906
$FF00
1904
$F000
1902

FIG. 19

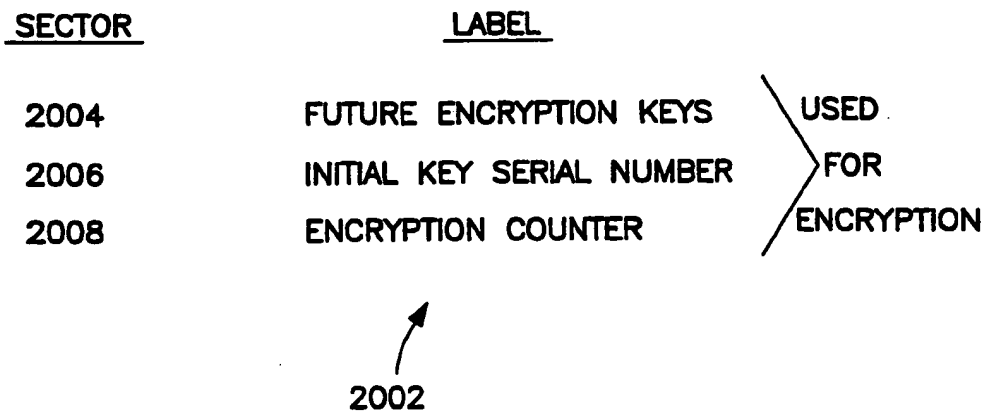

SECTOR
LABEL
2004
FUTURE ENCRYPTION KEYS
2006
INITIAL KEY SERIAL NUMBER
2008
ENCRYPTION COUNTER
USED FOR ENCRYPTION
2002

FIG. 20

FIG. 22

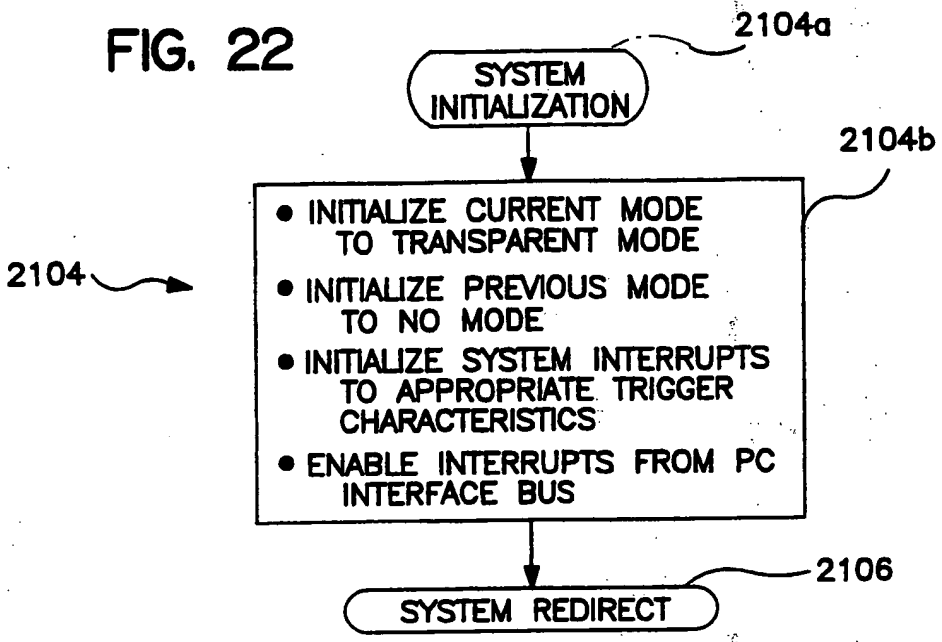

2104a
SYSTEM INITIALIZATION
2104b
• INITIALIZE CURRENT MODE TO TRANSPARENT MODE
• INITIALIZE PREVIOUS MODE TO NO MODE
• INITIALIZE SYSTEM INTERRUPTS TO APPROPRIATE TRIGGER CHARACTERISTICS
• ENABLE INTERRUPTS FROM PC INTERFACE BUS
2104
2106
SYSTEM REDIRECT

FIG. 24

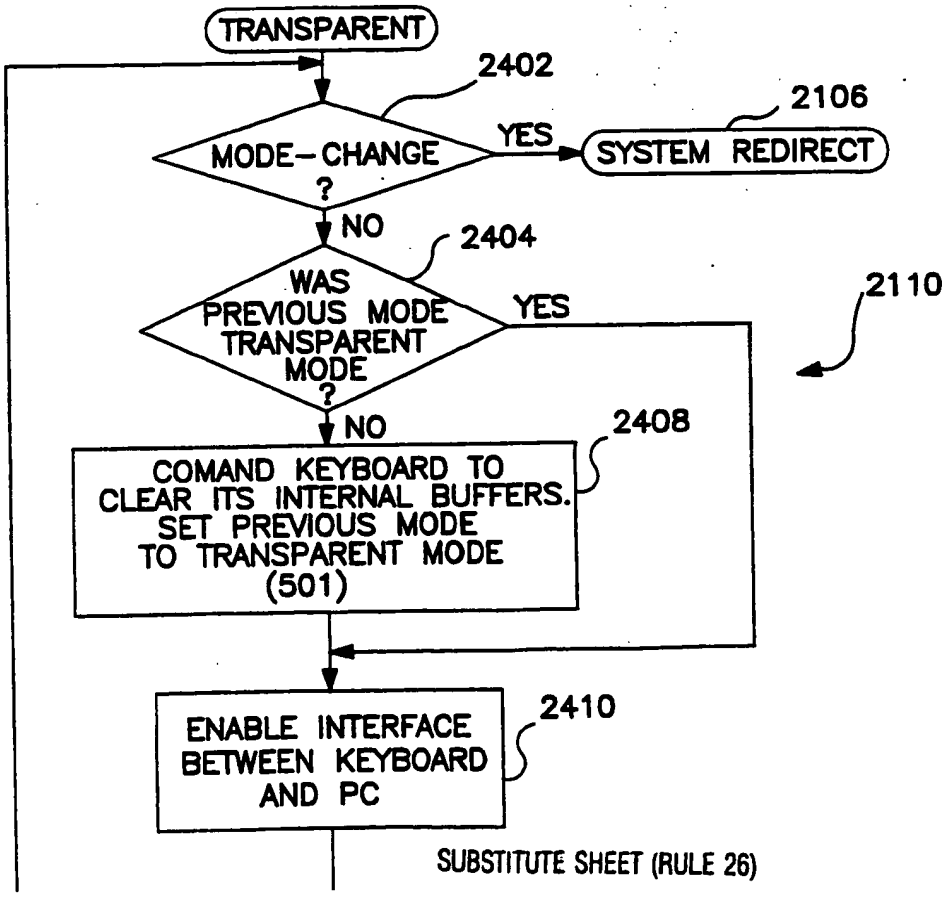
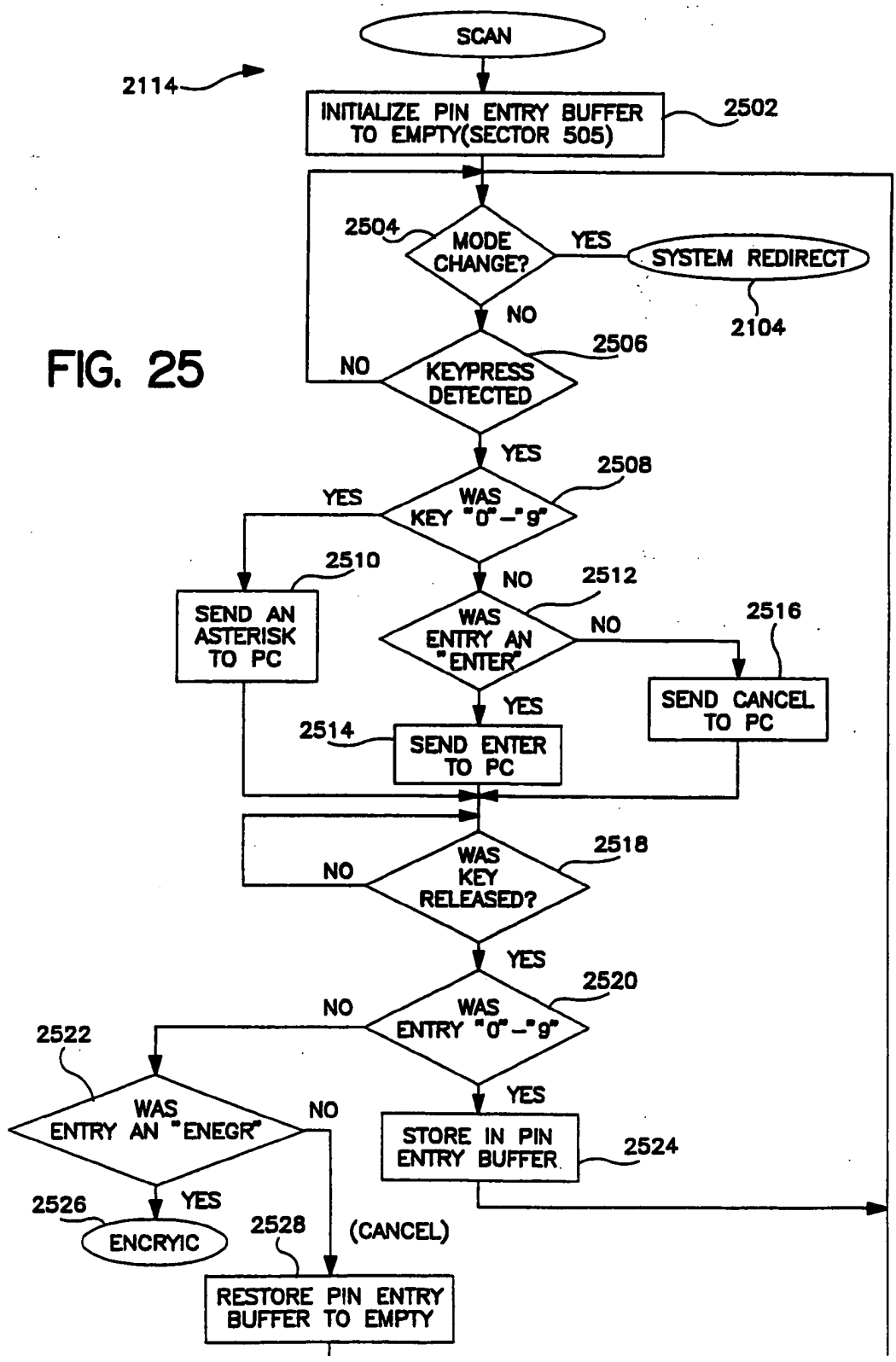

TRANSPARENT
2402
MODE-CHANGE ?
YES
2106
SYSTEM REDIRECT
NO
2404
WAS PREVIOUS MODE TRANSPARENT MODE ?
YES
2110
NO
2408
COMAND KEYBOARD TO CLEAR ITS INTERNAL BUFFERS. SET PREVIOUS MODE TO TRANSPARENT MODE (501)
2410
ENABLE INTERFACE BETWEEN KEYBOARD AND PC

FIG. 25


SCAN
2114
INITIALIZE PIN ENTRY BUFFER TO EMPTY(SECTOR 505)
2502
2504
MODE CHANGE?
YES
SYSTEM REDIRECT
2104
NO
2506
NO
KEYPRESS DETECTED
YES
2508
YES
WAS KEY "0"–"g"
2510
SEND AN ASTERISK TO PC
NO
2512
WAS ENTRY AN "ENTER"
NO
2516
SEND CANCEL TO PC
YES
2514
SEND ENTER TO PC
2518
NO
WAS KEY RELEASED?
YES
2520
NO
WAS ENTRY "0"–"g"
2522
YES
STORE IN PIN ENTRY BUFFER
2524
WAS ENTRY AN "ENEGR"
NO
2526
YES
ENCRYIC
2528
(CANCEL)
RESTORE PIN ENTRY BUFFER TO EMPTY

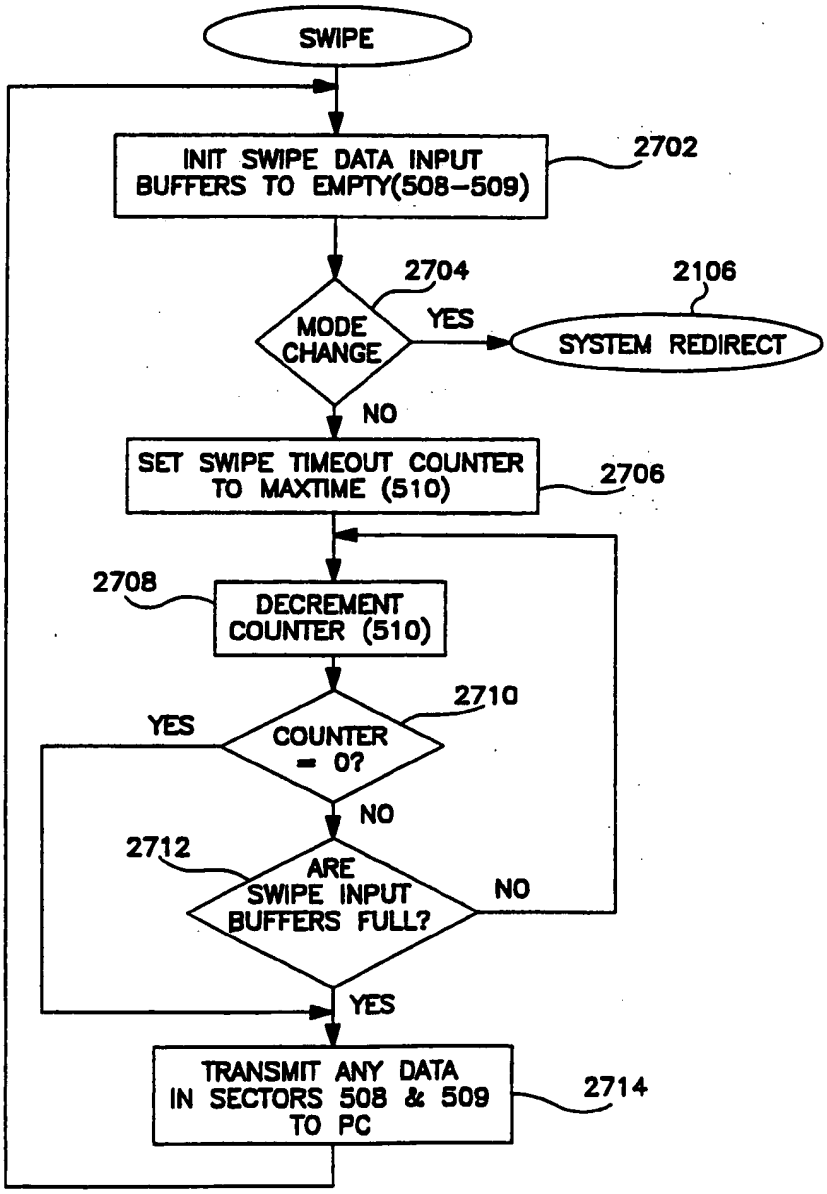

SWIPE
INIT SWIPE DATA INPUT BUFFERS TO EMPTY(508–509)
2702
2704
MODE CHANGE
YES
2106
SYSTEM REDIRECT
NO
SET SWIPE TIMEOUT COUNTER TO MAXTIME (510)
2706
2708
DECREMENT COUNTER (510)
2710
YES
COUNTER = 0?
NO
2712
ARE SWIPE INPUT BUFFERS FULL?
NO
YES
TRANSMIT ANY DATA IN SECTORS 508 & 509 TO PC
2714

FIG. 27

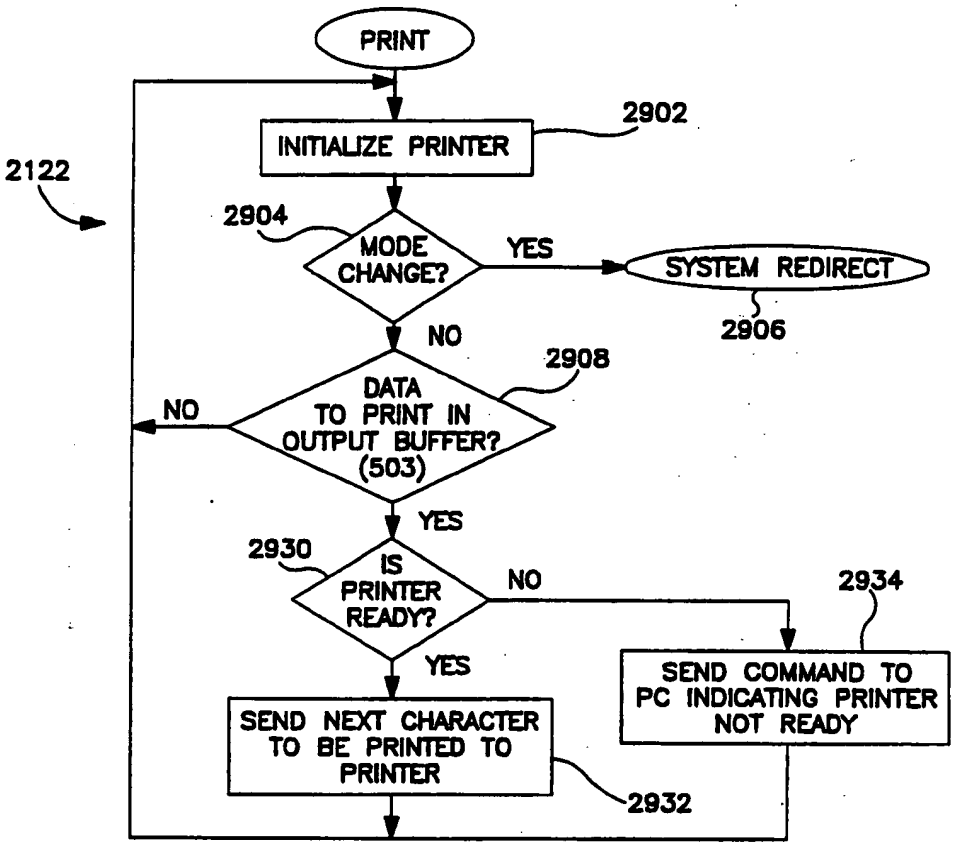

PRINT
INITIALIZE PRINTER
2902
2122
2904
MODE CHANGE?
YES
SYSTEM REDIRECT
2906
NO
2908
DATA TO PRINT IN OUTPUT BUFFER? (503)
NO
YES
2930
IS PRINTER READY?
NO
2934
YES
SEND COMMAND TO PC INDICATING PRINTER NOT READY
SEND NEXT CHARACTER TO BE PRINTED TO PRINTER
2932

FIG. 29

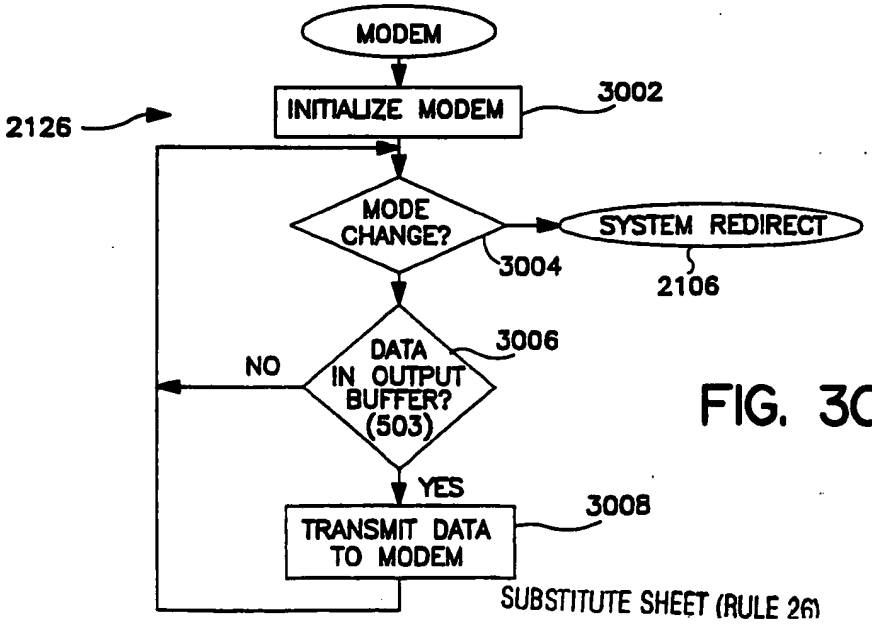

MODEM
INITIALIZE MODEM
3002
2126
MODE CHANGE?
SYSTEM REDIRECT
3004
2106
3006
DATA IN OUTPUT BUFFER? (503)
NO
YES
3008
TRANSMIT DATA TO MODEM

FIG. 30

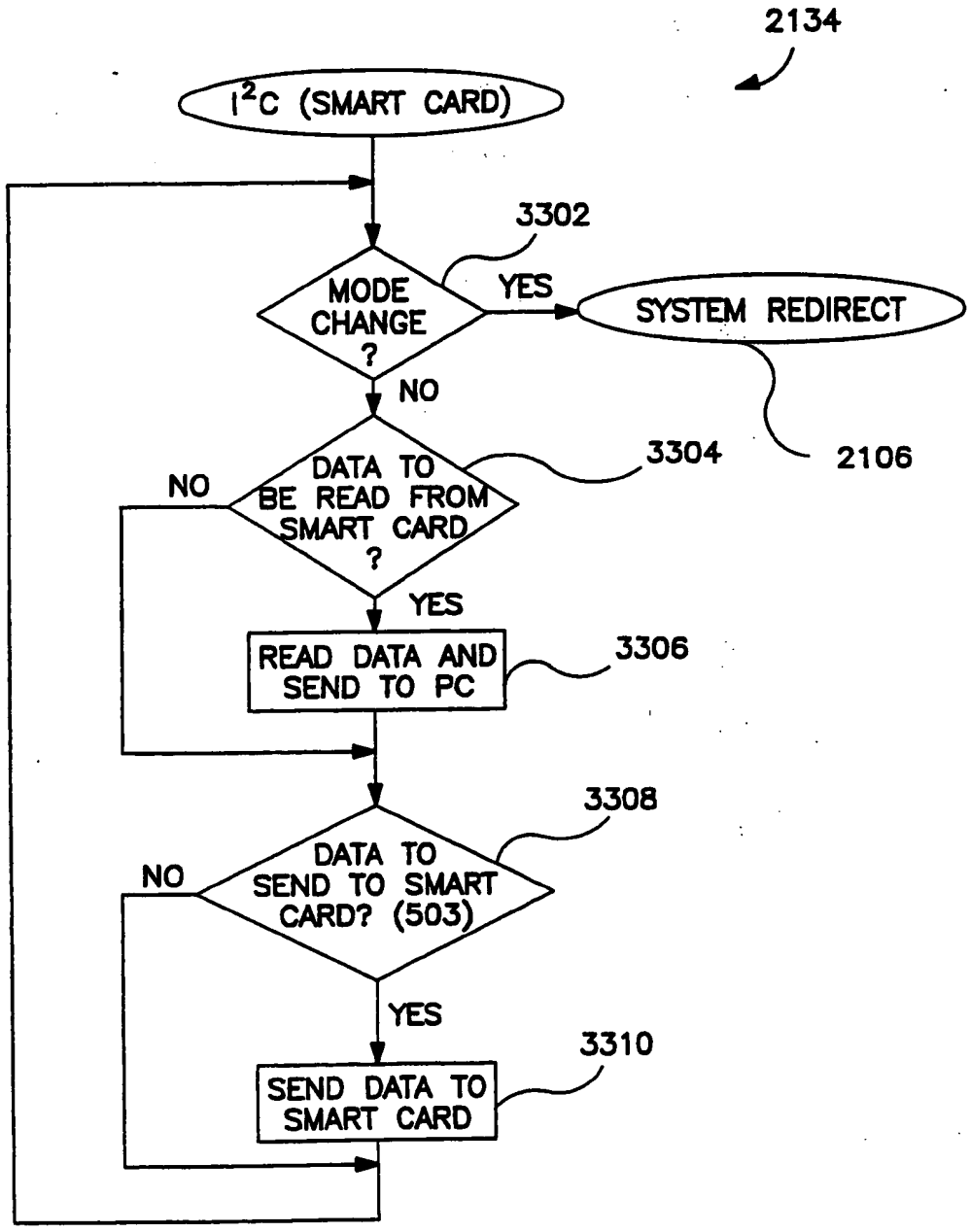

2134
I²C (SMART CARD)
3302
MODE CHANGE ?
YES
SYSTEM REDIRECT
2106
NO
3304
DATA TO BE READ FROM SMART CARD ?
NO
YES
READ DATA AND SEND TO PC
3306
3308
DATA TO SEND TO SMART CARD? (503)
NO
YES
3310
SEND DATA TO SMART CARD

FIG. 33

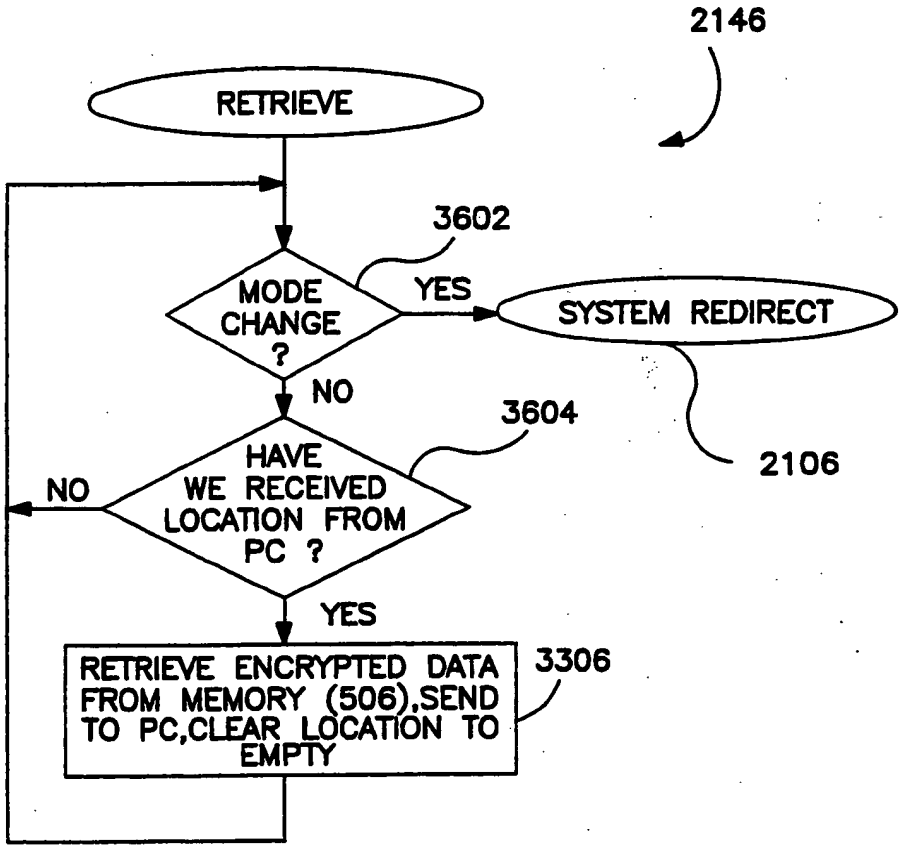

2146
RETRIEVE
3602
MODE CHANGE ?
YES
SYSTEM REDIRECT
2106
NO
3604
HAVE WE RECEIVED LOCATION FROM PC ?
NO
YES
RETRIEVE ENCRYPTED DATA FROM MEMORY (506),SEND TO PC,CLEAR LOCATION TO EMPTY
3306

FIG. 36